NetIQ® Identity Manager

Administrator's Guide to Configure Auditing

October 2019

Legal Notice

Contents

About this Book and the Library

The *Identity Manager - Administrator's Guide to Configure Auditing* provides the information necessary to set up Identity Manager components for auditing events. You can then integrate NetIQ Sentinel with Identity Manager to provide auditing and reporting services.

Intended Audience

This book provides information for individuals responsible for understanding administration concepts and implementing a secure, distributed administration model.

Other Information in the Library

For more information about the library for Identity Manager, see the Identity Manager documentation website.

About NetIQ Corporation

We are a global, enterprise software company, with a focus on the three persistent challenges in your environment: Change, complexity and risk—and how we can help you control them.

Our Viewpoint

Adapting to change and managing complexity and risk are nothing new

In fact, of all the challenges you face, these are perhaps the most prominent variables that deny you the control you need to securely measure, monitor, and manage your physical, virtual, and cloud computing environments.

Enabling critical business services, better and faster

We believe that providing as much control as possible to IT organizations is the only way to enable timelier and cost effective delivery of services. Persistent pressures like change and complexity will only continue to increase as organizations continue to change and the technologies needed to manage them become inherently more complex.

Our Philosophy

Selling intelligent solutions, not just software

In order to provide reliable control, we first make sure we understand the real-world scenarios in which IT organizations like yours operate — day in and day out. That's the only way we can develop practical, intelligent IT solutions that successfully yield proven, measurable results. And that's so much more rewarding than simply selling software.

Driving your success is our passion

We place your success at the heart of how we do business. From product inception to deployment, we understand that you need IT solutions that work well and integrate seamlessly with your existing investments; you need ongoing support and training post-deployment; and you need someone that is truly easy to work with — for a change. Ultimately, when you succeed, we all succeed.

Our Solutions

- Identity & Access Governance
- Access Management
- Security Management
- Systems & Application Management
- Workload Management
- Service Management

Contacting Sales Support

For questions about products, pricing, and capabilities, contact your local partner. If you cannot contact your partner, contact our Sales Support team.

Worldwide:	www.netiq.com/about_netiq/officelocations.asp
United States and Canada:	1-888-323-6768
Email:	info@netiq.com
Web Site:	www.netiq.com

Contacting Technical Support

For specific product issues, contact our Technical Support team.

Worldwide:	www.netiq.com/support/contactinfo.asp
North and South America:	1-713-418-5555
Europe, Middle East, and Africa:	+353 (0) 91-782 677
Email:	support@netiq.com
Web Site:	www.netiq.com/support

Contacting Documentation Support

Our goal is to provide documentation that meets your needs. If you have suggestions for improvements, click **Add Comment** at the bottom of any page in the HTML versions of the documentation posted at www.netiq.com/documentation. You can also email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

Contacting the Online User Community

Qmunity, the NetIQ online community, is a collaborative network connecting you to your peers and NetIQ experts. By providing more immediate information, useful links to helpful resources, and access to NetIQ experts, Qmunity helps ensure you are mastering the knowledge you need to realize the full potential of IT investments upon which you rely. For more information, visit http://community.netiq.com.

1 Overview

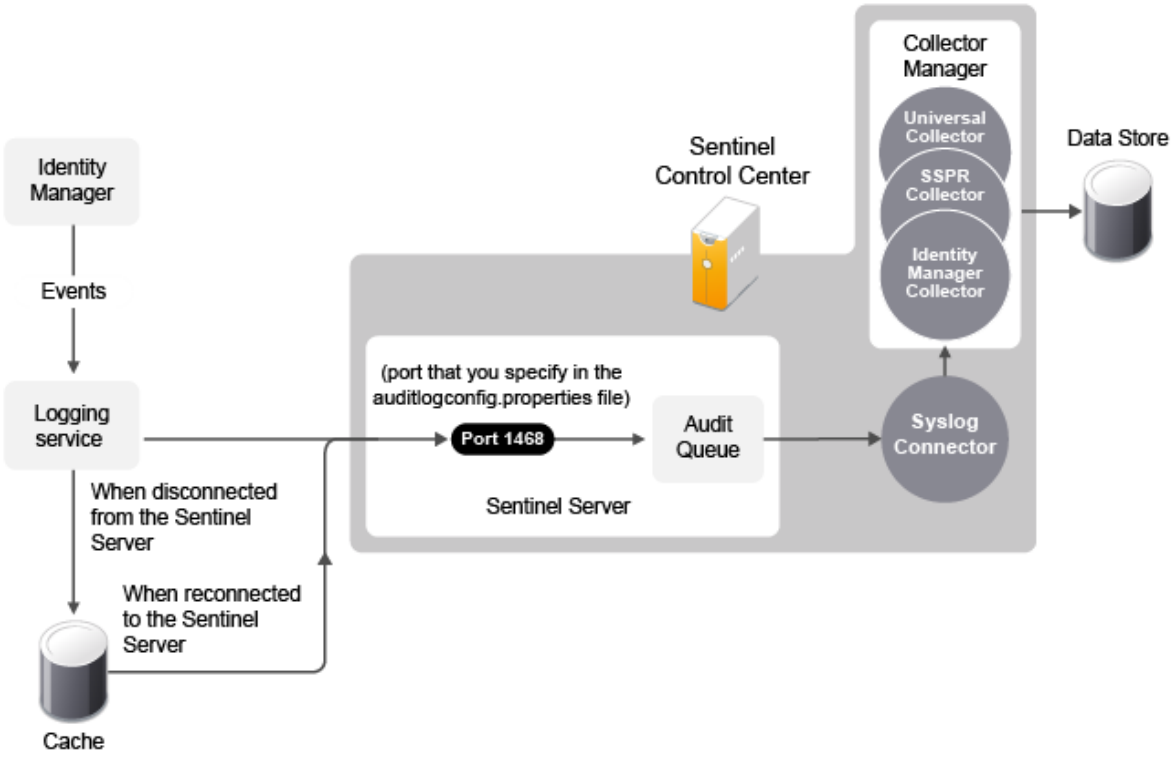
This guide helps you in implementing a uniform auditing across Identity Manager.

Identity Manager Auditing Architecture

This section explains how different components work together to provide a uniform auditing infrastructure in Identity Manager.

Identity Manager provides event forwarding capabilities to Security Event Log Management solutions such as Sentinel and ArcSight. Sentinel is the preferred audit event destination for Identity Manager. The following diagram illustrates how Identity Manager is configured with Sentinel Event Source Management (ESM).

Figure 1-1 *Auditing through CEF*



1. An Identity Manager event occurs and it is sent to the logging services.
2. (Conditional) If the logging services cannot connect to the Sentinel Server, the events are stored in cache until the connection is reestablished.
3. The logging services sends the events to the Sentinel Server, which stores the events in the audit queue.
4. The events in the audit queue are sent to the Syslog Connector.

5. The Syslog Connector sends the events to the Universal CEF Collector, which parses the information and then stores the parsed events in the data store.
6. (Optional) The stored events can be used for reports.

Audit Format Type

IMPORTANT: Auditing with NAudit and XDAS for the Identity Manager components is discontinued from Identity Manager 4.8. If you were using XDAS and NAudit with any previous version of Identity Manager, you must use only CEF for auditing purposes going forward.

Previous versions of Identity Manager used a combination of different auditing solutions. Identity Manager now supports Common Event Format (CEF) to provide a uniform auditing solution across all Identity Manager components.

The following table lists the availability of CEF in each Identity Manager version.

Identity Manager Version	Sentinel Collector Supported	Availability of Common Event Format (CEF)
4.6.x, where x is 0 to 4	NA	No
4.7 and 4.7.1	NetIQ Identity Manager collector	Yes
4.7.2 onward	Universal Common Event Format collector	Yes
4.8	Universal Common Event Format collector	Yes

Enabling Auditing

Auditing is not enabled by default. You must enable it after you have installed the Identity Manager components. NetIQ provides different auditing options for Identity Manager components as listed in the following table:

Table 1-1 *Identity Manager Auditing Support*

Component	Auditing Support
Identity Manager Engine, Remote Loader, Fanout Agent, Identity Applications, OSP, Identity Reporting, and Data Collection Services	To enable CEF auditing for these components, see “Setting up CEF Configuration” on page 19.
Identity Vault	To enable CEF auditing for Identity Vault, see Auditing with CEF in the *NetIQ eDirectory Administration Guide*
SSPR	To enable CEF auditing for SSPR, see Auditing for Self-Service Password Reset in the *Self Service Password Reset Administration Guide*.

Considerations for Migrating to CEF

To begin with the migration, you must first review the following considerations:

- Your current Identity Manager version.
- Your existing auditing configuration, that is, whether auditing is enabled or disabled.

NOTE: Auditing with NAudit and XDAS is discontinued from Identity Manager 4.8 release. If your auditing format type is not configured as CEF, then you may lose the audit events during migration to CEF format in Identity Manager 4.8.

The following table provides procedures to help you with the migration to CEF format. Select the procedure from this list depending on your current Identity Manager version and the existing auditing configuration.

Current Identity Manager Version	Existing Auditing Configuration	Required Action		
		Pre-Upgrade Steps	Upgraded Version	Post-Upgrade Steps
4.6.x, where x is 0 to 4	NA	None	Upgrade Identity Manager to 4.8.	1. Install and configure the NetIQ Sentinel Universal CEF Collector. For more information, see “Installing and Configuring the Universal CEF Collector” on page 15. 2. Configure Identity Manager components to use Common Event Format (CEF). For more information, see “Configuring Identity Manager Components to Log Audit Events in CEF Format” on page 19.

Current Identity Manager Version	Existing Auditing Configuration	Required Action		
		Pre-Upgrade Steps	Upgraded Version	Post-Upgrade Steps
4.7.x, where x is 0 to 4	If CEF auditing is disabled.	None	Upgrade Identity Manager to 4.8.	1. Install and configure the NetIQ Sentinel Universal CEF Collector. For more information, see “Installing and Configuring the Universal CEF Collector” on page 15. 2. Configure Identity Manager components to use Common Event Format (CEF). For more information, see “Configuring Identity Manager Components to Log Audit Events in CEF Format” on page 19.
4.7.x, where x is 0 and 1	If CEF auditing is enabled.	Install and configure the NetIQ Sentinel Universal CEF Collector. For more information, see “Installing and Configuring the Universal CEF Collector” on page 15.	Upgrade Identity Manager to 4.8.	Configure Identity Applications to use Common Event Format (CEF). For more information, see “Configuring Identity Applications” on page 22.
4.7.x, where x is 2 and above	If CEF auditing is enabled.	None	Upgrade Identity Manager to 4.8.	Configure Identity Applications to use Common Event Format (CEF). For more information, see “Configuring Identity Applications” on page 22.
4.8	Identity Manager is freshly installed.	None	Upgrade Identity Manager to 4.8.	Install and configure Sentinel with Identity Manager. For more information, see Chapter 2, “Configuring NetIQ Sentinel with Identity Manager,” on page 13.

2 Configuring NetIQ Sentinel with Identity Manager

Use the following checklist to verify that all of the steps are completed to install and configure Sentinel with Identity Manager.

- ❒ Install and configure Sentinel. NetIQ recommends that you install Identity Manager and Sentinel on different servers. For more information, see the *NetIQ Sentinel Installation Guide*.
- ❒ Install and configure the NetIQ Sentinel Universal CEF Collector. For more information, see Chapter 3, “Installing and Configuring the Sentinel Collectors,” on page 15.
- ❒ Install and configure the Syslog Connector. For more information, see Chapter 4, “Installing the Syslog Connector,” on page 17.
- ❒ Configure Identity Manager components to use Common Event Format (CEF).

  For more information, see Chapter 5, “Configuring Identity Manager Components to Log Audit Events in CEF Format,” on page 19.
- ❒ Configure the Sentinel Control Center to access the predefined reports for Identity Manager.

3 Installing and Configuring the Sentinel Collectors

You must install and configure the Sentinel collectors which will parse and normalize the raw data to the respective connectors and then convert the data into a Sentinel event.

The collectors must be added to the Event Source Manager to be installed. This step is only done once. The added collectors are then displayed during configuration.

NOTE: After fresh installation of Sentinel with the required collectors and connectors installed and configured, restart Sentinel for the changes to take effect.

Installing and Configuring the Universal CEF Collector

The Universal CEF Collector parses non-event data and transform the raw scan data into a format understood by Sentinel. Sentinel then stores the vulnerability data in the database and includes it in the Exploit Detection map. For more detailed information about Sentinel collectors, see the Sentinel Collector Script User's Guide.

To install the Universal CEF Collector,

1. Download the latest Universal CEF Collector (`.zip` file) from the NetIQ Sentinel Plug-ins website.
2. Log in to the Sentinel Control Center.
3. Select the **Event Source Management** > **Live View**, then select **Tools** > **Import plugin**.
4. Browse to and select the `.zip` file you just downloaded, then click **Next**.
5. Follow the remaining prompts, then click **Finish**.

The Universal CEF Collector must be configured to work. To configure the Universal CEF Collector,

1. In the Event Source Management live view, right-click **Sentinel Server**, then click **Add Collector**.
2. Select **Universal** in the **Vendor** column.
3. Select **Common Event Format** in the **Name** column, then click **Next**.
4. From the **Installed Collectors** column, select **Universal_Common-Event-Format_Collector_Version**, then click **Next**. For example, `Universal Common Event Format 2011.1r4`.
5. Follow the prompts and click **Finish**.

The next step is to proceed to Chapter 4, "Installing the Syslog Connector," on page 17.

Installing and Configuring the SSPR Collectors

To install the SSPR Collector,

1. Download the latest SSPR Collector (`.zip` file) from the NetIQ Plug-ins website.
2. Log in to the Sentinel Control Center.
3. Select the **Event Source Management** > **Live View**, then select **Tools** > **Import plugin**.
4. Browse to and select the `.zip` file you just downloaded, then click **Next**.
5. Follow the remaining prompts, then click **Finish**.

The SSPR Collector must be configured to work. To configure the SSPR Collector,

1. In the Event Source Management live view, right-click **Sentinel Server**, then click **Add Collector**.
2. Select **NetIQ** in the **Vendor** column.
3. Select **Identity Manager** in the **Name** column, then click **Next**.
4. From the **Installed Collectors** column, select **<Collector>_<Collector_*Version*>**, then click **Next**.

   For example: **SelfServicePasswordReset_<Collector_*Version*>**
5. Follow the prompts and click **Finish**.

For SSPR, the next step is to proceed to “Installing and Configuring the Syslog Connector” on page 17.

4 Installing the Syslog Connector

The Syslog Connector facilitates integration between Identity Manager and Sentinel. You must install and configure the Universal CEF Collector before you install and configure the Syslog Connector.

NOTE: After installing Sentinel with the required collectors and connectors installed and configured, restart Sentinel for the changes to take effect.

Installing and Configuring the Syslog Connector

To set up the connection with the Event Source, you must install the Syslog Connector plug-in.

Perform the following actions to install the Syslog Connector plug-in:

1. Download the latest Syslog Connector (`.zip` file) from the Sentinel Plug-ins website. The Syslog Connector is located under the **Connectors** tab. Save the file to the local computer where you want to run Event Source Management.
2. Log in to the Sentinel Control Center.
3. Go to the **Event Source Management** menu, and select the **Live View** option. For more information, see Configuring Data Collection for Syslog Event Sources in the *Sentinel Administration Guide*.
4. Select **Tools > Import plug-in** to display the Plug-in Import Type window.
5. In the Plug-in Import Type window, select the **Import Collector or Connector plug-in package file (.zip, .clz, .cnz)** option.
6. Click **Next**.
7. In the Choose Plug-in Package File window, browse to and select the Connector file you just downloaded.
8. Follow the remaining Import Plug-In Wizard instructions to import the Connector into the plug-in repository.

   If another version of this Connector is already in use, you can click **View Deployed Plug-ins** to see which Event Source objects use the deployed Connectors.
9. (Optional) To update the deployed Connectors, select **Update Deployed Plug-ins**.
10. Click **Finish**.

5 Configuring Identity Manager Components to Log Audit Events in CEF Format

Identity Manager introduces Common Event Format (CEF), an open log management standard for auditing events across all Identity Manager components. CEF enables you to use a common event log format so that auditing data can easily be collected and aggregated for further analysis. CEF uses the Syslog message format as a transport mechanism.

Advantages of CEF

Previous versions of Identity Manager used a combination of different auditing solutions. Identity Manager now supports CEF to provide a uniform auditing solution across all Identity Manager components that can help improve your experience of configuring and working with auditing.

CEF uses a standard Syslog message format that simplifies log management. This enables you to integrate disparate Identity Manager data in your enterprise. The new event format seamlessly integrates with Sentinel.

Setting up CEF Configuration

After you install Identity Manager, ensure that all Identity Manager components are configured to generate the CEF events. To configure the components, see the following sections:

- “Configuring Identity Manager Engine” on page 20
- “Configuring Remote Loader” on page 20
- “Configuring .NET Remote Loader” on page 21
- “Configuring Java Remote Loader” on page 21
- “Configuring Fanout Agent” on page 22
- “Configuring Identity Applications” on page 22
- “Configuring Identity Reporting” on page 24
- “Configuring Data Collection Services” on page 25
- “Configuring One SSO Provider” on page 26
- “Configuring Self Service Password Reset” on page 27

IMPORTANT: If Identity Manager loses communication with the Sentinel server, Java Remote Loader, Fanout agent, and DCS events are not logged in the cache file for an approximate duration of two minutes. After the connection is restored, any cached events are sent to Sentinel after a delay of two minutes. There is no loss of events when Sentinel is normally shut down.

The CEF configuration settings are stored in a simple, text-based files for each component. For more information, see Understanding the Properties Files for CEF Auditing.

Before configuring the Identity Manager components, ensure that the Universal CEF Collector is configured in the Sentinel server. To log events with Universal CEF collector, ensure that the collector version is latest. For information about installing and configuring the Universal CEF collector, see Installing and Configuring the Sentinel Collectors.

Configuring Identity Manager Engine

The Identity Manager engine provides events for auditing. The configuration settings for Identity Manager Engine is stored in the `auditlogconfig.properties.template` file.

Perform the following steps to configure settings for enabling CEF auditing:

1. Log in to the server where Identity Manager Engine is installed.
2. Navigate to the directory where the `auditlogconfig.properties.template` file is present. By default, the file is located in the following directory:

   Linux: `/etc/opt/novell/eDirectory/conf/`

   Windows: `<eDirectory_install_path>\eDirectory\Conf`
3. Rename the `auditlogconfig.properties.template` file as `auditlogconfig.properties`.
4. Edit the `auditlogconfig.properties` file. Uncomment and update the appenders by removing # before each property. For more information, see "Identity Manager Engine, Remote Loader, and .NET Remote Loader" on page 51 in *Understanding the auditlogconfig.properties File* section.
5. Restart the Identity Vault.

To select events for auditing in CEF, use iManager.

1. Log in to iManager.
2. Select **Identity Manager Administration** > **Identity Manager Overview**.
3. Browse to and select the driver set object that contains the driver.
4. Select the driver set objects that contains the driver.
5. Click **Driver Set** and then click **Edit Driver Set properties**.
6. Click the **Log Level** tab, select the **Log specific events** radio button, and then click  .
7. Select the events you want to log and click **OK**.

For the list of Identity Manager engine events, see Engine Events.

Configuring Remote Loader

The configuration settings for Remote Loader is stored in the `auditlogconfig.properties.template` file.

NOTE: CEF logging in Remote Loader will be enabled only if the `auditlogconfig.propertes` file exists.

Perform the following steps to configure settings for enabling CEF auditing:

1. Log in to the server where Remote Loader is installed.
2. Navigate to the directory where the `auditlogconfig.properties.template` file is present. By default, the file is located in the following directory:

Linux: `/etc/opt/novell/eDirectory/conf/`

Windows: `<remote_loader_installted_location>\<processor_type>\`

3. Rename the `auditlogconfig.properties.template` file as `auditlogconfig.properties`.
4. Edit the `auditlogconfig.properties` file. Uncomment and update the appenders by removing # before each property. For more information, see "Identity Manager Engine, Remote Loader, and .NET Remote Loader" on page 51 in *Understanding the auditlogconfig.properties File* section.
5. Restart Tomcat service.

For the list of Remote Loader events, see Remote Loader Events.

Configuring .NET Remote Loader

The configuration settings for .NET Remote Loader is stored in the `auditlogconfig.properties.template` file.

NOTE: The .NET Remote Loader is applicable for Windows only.

Perform the following steps to configure settings for enabling CEF auditing:

1. Log in to the server where .NET Remote Loader is installed.
2. Navigate to the directory where the `auditlogconfig.properties.template` file is present. By default, the file is located at:

   `products\IDM\windows\setup\remoteloader.NET`
3. Rename the `auditlogconfig.properties.template` file as `auditlogconfig.properties`.
4. Edit the `auditlogconfig.properties` file. Uncomment and update the appenders by removing # before each property. For more information, see "Identity Manager Engine, Remote Loader, and .NET Remote Loader" on page 51 in *Understanding the auditlogconfig.properties File* section.
5. Restart Tomcat service.

Configuring Java Remote Loader

NOTE: Ensure that the Rolling File Appender directory is present in `/var/opt/novell/eDirectory/log/cef-events.log` location for Java Remote Loader. Otherwise, Rolling File Appender directory will not work and no events will be logged.

The configuration settings for Java Remote Loader is stored in the `auditlogconfig.properties.template` file.

Perform the following steps to configure settings for enabling CEF auditing:

1. Log in to the server where Java Remote Loader is installed.
2. Navigate to the directory where the `auditlogconfig.properties.template` file is present. By default, the file is located at:

   Linux: `<extracted loc of dirxml_jremote.tar.gz>/doc`

   `dirxml_jremote.tar.gz` is located at `IDM/packages/java_remoteloader`

   Windows: `<extracted loc of dirxml_jremote.tar.gz>/doc`

`dirxml_jremote.tar.gz` is located at `products/IDM/java_remoteloader`

3. Rename the `auditlogconfig.properties.template` file as `auditlogconfig.properties`.
4. Edit the `auditlogconfig.properties` file. Uncomment and update the appenders by removing # before each property. For more information, see "Java Remote Loader and Fanout Agent" on page 54 in *Understanding the auditlogconfig.properties File* section.
5. To run the Java Remote Loader, specify the following command:

   ```
   dirxml_jremote -config <Remote Loader configuration file> -auditlogfile /<PATH of the directory where auditlogconfig.properties file is located>/auditlogconfig.properties
   ```

6. Restart Tomcat service.

For a list of Java Remote Loader events, see Remote Loader Events.

Configuring Fanout Agent

NOTE: Ensure that the Rolling File Appender directory is present in `/var/opt/novell/eDirectory/log/cef-events.log` location for Fanout Agent. Otherwise, Rolling File Appender directory will not work and no events will be logged.

When you run the Fanout agent for the first time, the `auditlogconfig.properties.template` file is created and located in the following directories:

Linux: `/opt/novell/dirxml/fanoutagent/config`

Windows: `<install-location>\FanoutAgent\config`

For the list of events, see Fanout Agent Events.

Configuring Identity Applications

To configure settings for enabling CEF auditing, perform the following steps:

1. Log in to the Identity Applications server.
2. Navigate to the directory where `idmuserapp_logging.xml` and `workflow_logging.xml` files are located.
   - **Linux:** `/opt/netiq/idm/apps/tomcat/conf`
   - **Windows:** `<apps_install_path>\idm\apps\tomcat\conf`

   NOTE

   - The `workflow_logging.xml` file is applicable for Identity Manager 4.8 version only.
   - By default, Identity Manager saves the logging configuration in `idmuserapp_logging.xml` file. However, the workflow events are generated only if CEF auditing is enabled in `workflow_logging.xml` file.

   ---

3. Add the CEF appenders and loggers in idmuserapp_logging.xml and workflow_logging.xml files. For more information, see "Understanding the idmuserapp_logging.xml File" on page 56 and "Understanding the workflow_logging.xml File" on page 58. NetIQ recommends you to retain the default value for the parameters in the appenders and loggers section.

NOTE: If you have upgraded to Identity Manager 4.8, you must ensure that all XDAS configuration and Naudit appenders and loggers have been deleted from the `idmuserapp_logging.xml` file.

4 (Conditional) Specify an intermediate event store directory to store and back up the events. Make sure that the permission and ownership are changed to *novlua* for that directory. To change the permission of the directory, run the following commands:

```
chown novlua:novlua <directory_path>
```

```
chmod 755 <directory_path>
```

where `<directory_path>` is path to the intermediate event store directory.

IMPORTANT: If you do not provide the required permissions to the intermediate event store directory, then:

- you may not be able to access Identity Applications.
- the OSP events will not be logged to the intermediate event store directory.

For Windows platform, provide the Administrative permission to the directory.

5 You can enable CEF auditing through either Identity Manager Dashboard or using configuration update utility.

To enable CEF auditing through Identity Manager Dashboard:

1. Log in to Identity Manager Dashboard as an administrator.
2. Select **Configuration** > **Logging**.
3. Click **Auditing Configuration** drop-down menu and select **Enable CEF format**. Specify the following auditing server details to use CEF format:

Fields	Description
Destination host	Specifies the destination hostname or IP address of the auditing server.
Destination port	Specifies the destination port number of the auditing server.
Network protocol	Specifies the protocol that should be used to establish communication with the auditing server. To establish a secure communication with the auditing server, select **TCP** protocol and enable **Use TLS** option. Provide the **Keystore file** name and the **Keystore password**.
Intermediate event store directory	Specifies the temporary directory where the events can be stored. This directory serves as a backup for an auditing server. If Identity Applications is freshly installed, the directory path will be populated by default. You can also provide path to intermediate event store directory of your choice. For more information, see Step 4.

4. Click **Apply**.

To enable CEF auditing through configuration update utility:

1. Navigate to the `/opt/netiq/idm/apps/configupdate` directory.
2. Run the following command: `./configupdate.sh`
3. In the **CEF Auditing** tab, select **Send audit events** check box and specify the following auditing server details to use CEF format:

Fields	Description
Destination host	Specifies the destination hostname or IP address of the auditing server.
Destination port	Specifies the destination port number of the auditing server.
Network protocol	Specifies the protocol that should be used to establish communication with the auditing server. To establish a secure communication with the auditing server, select **TCP** protocol and enable **Use TLS** option. Provide the **Keystore file** name and the **Keystore password**.
Intermediate event store directory	Specifies the temporary directory where the events can be stored. This directory serves as a backup for an auditing server. If Identity Applications is freshly installed, the directory path will be populated by default. You can also provide path to intermediate event store directory of your choice. For more information, see Step 4.

4. Click **OK**.

6 Restart Tomcat.

For the list of identity applications events, see Identity Applications Events.

Configuring Identity Reporting

The configuration settings for Identity Reporting auditing is stored in the `idmrptcore_logging.xml` file.

NOTE: You must use Sentinel 8.2 (or later) and Universal CEF collector version 2011.1r4 (or later) to log the events.

Perform the following steps to configure settings for enabling CEF auditing:

1 Log in to the server where you have installed Identity Reporting.

2 Navigate to the directory where `idmrptcore_logging.xml` file is present. By default, the file is located in the following directories:

Linux: `/opt/netiq/idm/apps/tomcat/conf`

Windows: `C:\netiq\idm\apps\tomcat\conf`

3 Add the following in the `idmrptcore_logging.xml` file:

```
<audit>
        <syslog>
            <enabled>true</enabled>
            <protocol>TCP</protocol>
            <host>IP Address of your auditing server</host>
            <port>Audting server port</port>
            <cache-dir>name of the cache directory</cache-dir>
            <cache-file>name of the cache file within the cache directory</
cache-file>
       <application>Reporting Core</application>
       <vendor>Micro Focus</vendor>
           <version>6.0</version>
        </syslog>
    </audit>
```

You must specify the Identity Reporting version number in the `<version>` element. For example, 6.0.

For sample `idmrptcore_logging.xml` file, see "Understanding the idmrptcore_logging.xml File" on page 61.

4 Restart Tomcat service.

For the list of Identity Reporting events, see Identity Reporting Events.

Configuring Data Collection Services

The configuration settings for DCS auditing is stored in the `idmrptdcs_logging.xml` file.

Perform the following steps to configure settings for enabling CEF auditing:

1 Log in to the server where Data Collection Services is running.

2 Navigate to the directory where `idmrptdcs_logging.xml` file is present. By default, the file is located in the following directories:

Linux: `/opt/netiq/idm/apps/tomcat/conf`

Windows: `C:\netiq\idm\apps\tomcat\conf`

3 Edit the `idmrptdcs_logging.xml` file. Uncomment and update the appenders by removing # before each property. For more information, see "Understanding the idmrptdcs_logging.xml File" on page 59.

4 Restart Tomcat service.

NOTE: You can define the Rolling File Appender directory and the cache directory. Make sure that you set the `novlua` permission for these directory, otherwise, Rolling File Appender or the cache directory will not work and no events will be logged. For example, you can change the permission and ownership of the directory using the `chown novlua:novlua /<directorypath>` command, where `<directorypath>` is the Rolling File Appender path or cache file directory path.

For a list of DCS events, see DCS Events.

Configuring One SSO Provider

When you have OSP and Identity Applications on the same server, the CEF auditing configuration performed on Identity Applications will apply to OSP (One SSO Provider) also. If OSP is installed on standalone server, then the configuration settings for OSP must be performed through the configuration update utility. For information on enabling CEF for OSP on Linux and Windows, see the following sections:

Linux

Launch the `configupdate.sh` from the `/opt/netiq/idm/apps/configupdate/` directory of the Identity Applications and define the values for the following CEF auditing parameters for the single sign-on client:

Send audit events

Specifies whether you want to use CEF for auditing events.

Destination host

Specifies the DNS name or the IP address of the auditing server.

Destination port

Specifies the port of the auditing server.

Network protocol

Specifies the network protocol used by the auditing server to receive CEF events.

Use TLS

Applies only when you want to use TCP as your network protocol.

Specifies if the auditing server is configured to use TLS with TCP. Select **Use TLS** > **Show Advanced Options**, and provide the **Identity Manager Keystore file name** and the I**dentity Manager Keystore password**.

Intermediate event store directory

Specifies the location of the cache directory before the CEF events are sent to the auditing server. If you are providing an intermediate event store directory of your choice, you must first ensure that the permission and ownership are set to `novlua` for that directory. To change the permission of the directory, run the following commands:

```
chown novlua:novlua <directory_path>
```

```
chmod 755 <directory_path>
```

where `<directory_path>` is the path to the intermediate event store directory.

Windows

Launch the `configupdate.bat` from the installation subdirectory for the Identity Applications (`C:\NetIQ\idm\apps\UserApplication`) and define the values for the following CEF Auditing parameters for the single sign-on client:

Send audit events

Specifies whether you want to use CEF for auditing events in Identity Applications.

Destination host

Specifies the DNS name or the IP address of the auditing server.

Destination port

Specifies the port of the auditing server.

Network Protocol

Specifies the network protocol used by the auditing server to receive CEF events.

Use TLS

Applies only when you want to use TCP as your network protocol.

Specifies if the auditing server is configured to use TLS with TCP.

Intermediate event store directory

Specifies the location of the cache directory before the CEF events are sent to the auditing server.

NOTE: Ensure that the `novlua` permissions are set for the Intermediate event store directory. Otherwise, you cannot access the IDMDash and IDMProv applications. Also, none of the OSP events will be logged in the Intermediate event store directory. For example, you can change the permission and ownership of the directory using the `chown novlua:novlua <directorypath>` command, where `<directorypath>` is the Intermediate event store directory.

Configuring Self Service Password Reset

For information on enabling CEF audit for SSPR, see Auditing for Self Service Password Reset in Self Service Password Reset Administration Guide.

6 Securing the Logging System

The Sentinel server and some of the Identity Manager components utilize embedded certificates generated by an internal Certificate Authority (CA). These SSL certificates ensure that communication between the Identity Manager instrumentation and the Sentinel server is secure.

Enabling SSL Connection for User Application

To create a SSL certificate, perform the following actions:

1. Download the public certificate in `.der` format from the Sentinel server.

   For example, if you are using Mozilla Firefox as your browser that already has a certificate, use the following procedure to download the certificate.

   1a Launch the Sentinel Server in your browser.

   1b Click **Show site information > View Certificate**.

   1c Go to **Details** tab and export the certificate in `.der` format.

2. Add the certificate to the Java keystore.

   For example, use the following command:

   ```
   keytool -import -file PATH_OF_DERFile\PublicKeyCert.der -keystore
   KEYSTOERPATH\NAME.keystore -storepass keystorepass
   ```

The next step is to define which events to log. Proceed to “Managing Identity Manager Events” on page 31.

Enabling SSL Connection for Identity Manager Engine

Perform the following steps to enable SSL connectivity for the Identity Manager Engine:

1. Login to the server where you have installed Identity Manager Engine.
2. Go to `/etc/opt/novell/eDirecotry/conf` folder.
3. Get the Sentinel Log Manager certificate and upload to keystore using the following command:

   ```
   echo | openssl s_client -connect <sentinel ip>:1443 2>&1 | sed -ne '/-BEGIN
   CERTIFICATE-/,/-END CERTIFICATE-/p' > slm.pem
   ```

4. Edit the `auditlogconfig.properties` file. You must uncomment and update the appenders in the `auditconfig.properties` file. You can uncomment by removing the # before each property. For more information, see “Understanding the auditlogconfig.properties File” on page 51.
5. Save the `auditconfig.properties` file and exit.
6. Select those events that you want to audit from the driver set properties in iManager. For more information, see “Selecting Events for the Driver Set” on page 32.
7. Restart Identity Vault using the following commands:

   ```
   ndsmanage stopall

   ndsmanage startall
   ```

7 Managing Identity Manager Events

The event information sent to NetIQ Sentinel is managed through product-specific instrumentations, or plug-ins. The Identity Manager Instrumentation allows you to configure which events are logged to your data store. You can select predefined log levels, or you can individually select the events you want to log. You can also add user-defined events to the Identity Manager schema.

The following sections review how to manage Identity Manager events:

Selecting Events to Log

The Identity Manager Instrumentation allows you to select events to be logged for the User Application, driver set, or a specific driver.

NOTE: Drivers can inherit logging configuration from the driver set.

Selecting Events for the User Application

The User Application enables you to change the log level settings of individual loggers and enable logging in Platform Agent and CEF format:

1. Log in to Identity Applications.
2. Select the **Application** tab.
3. Select the **Navigation and Access** link.
4. Click **Application Configuration** and then click **Logging**.
5. Select one of the following log levels for the listed logs.

Log Level	Description
Fatal	Writes Fatal level messages to the log.
Error	Writes Fatal and Error level messages to the log.
Warn	Writes Fatal, Error, and Warn level messages to the log.
Info	Writes Fatal, Error, Warn, and Info level messages to the log.
Debug	Writes Fatal, Error, Warn, Info, and debugging information to the log.
Trace	Writes Fatal, Error, Warn Info, debugging, and tracing information to the log.

6 Select **Enable CEF format** check box if you want to log the events in CEF format.

For this option to work, you must add the Syslog appender in the `idmuserapplogging.xml` file during the installation of the User Application. For more information, see Section 5, “Configuring Identity Manager Components to Log Audit Events in CEF Format,” on page 19.

7 To save the changes for any subsequent application server restarts, select **Persist the logging changes**.

8 Click **Submit**.

The User Application logging configuration is saved in `/opt/netiq/idm/apps/tomcat/conf/idmuserapp_logging.xml`.

Selecting Events for the Driver Set

1 In iManager, select **Identity Manager > Identity Manager Overview**.

2 Browse to and select the driver set object.

3 Click the driver set object in the list of driver sets, then click **Driver Set > Edit Driver Set properties**.

4 Click the **Log Level** tab, then select a log level for the driver set.

For an explanation of each log level, see Table 7-1, “Identity Manager Log Levels,” on page 33.

5 Enable the **Turn off logging to Driver Set, Subscriber and Publisher logs** option to prevent logging audit events to eDirectory.

Enabling this option improves the performance of the Identity Manager system.

6 Click **Apply** or **OK** to save your changes.

NOTE: Changes to configuration settings are logged by default.

Selecting Events for a Specific Driver

1 In iManager, select **Identity Manager > Identity Manager Overview**.

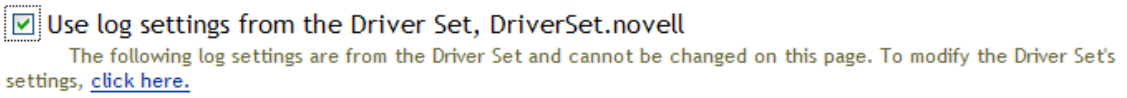
2 Browse to and select the driver set object that contains the driver

3 Select the driver set from the list of driver sets.

4 Click the upper right corner of the driver icon, then select **Edit properties**.

5 Select the **Log Level** tab.

6 (Optional) By default, the Driver object is configured to inherit log settings from the Driver Set object. To select logged events for this driver only, deselect **Use log settings from the Driver Set**.



7 Enable the **Turn off logging to Driver Set, Subscriber and Publisher logs** option.

Enabling this option improves the performance of the Identity Manager system.

8 Select a log level for the current driver.

For an explanation of each log level, see Table 7-1, “Identity Manager Log Levels,” on page 33.

9 Click **Apply** or **OK** to save your changes.

NOTE: Changes to configuration settings are logged by default.

Identity Manager Log Levels

The following table provides an explanation of the Identity Manager Instrumentation log levels:

Table 7-1 *Identity Manager Log Levels*

Option	Description
Log errors	This is the default log level. The Identity Manager Instrumentation logs user-defined events and all events with an error status. You receive only events with a decimal ID of 196646 and an error message stored in the Text1 field.
Log errors and warnings	The Identity Manager Instrumentation logs user-defined events and all events with an error or warning status. You receive only events with a decimal ID of 196646 or 196647 and an error or warning message stored in the first text field.
Log specific events	This option allows you to select the Identity Manager events you want to log. Click  to select the specific events you want to log. After you select the events you want to log, click **OK**. For a list of all available events, see Appendix A, “Identity Manager Events,” on page 41.
Only update the last log time	The Identity Manager Instrumentation logs only user-defined events. When an event occurs, the last log time is updated so you can view the time and date of the last error in the status log.
Logging off	The Identity Manager Instrumentation logs only user-defined events.
Turn off logging to DriverSet, Subscriber and Publisher logs	Turns off logging to the Driver Set object, Subscriber, and Publisher logs.

Option	Description
Maximum Number of Entries in the Log	This setting allows you to specify the maximum number of entries to log in the status logs.

User-Defined Events

Identity Manager enables you to configure your own events to log to NetIQ Sentinel. Events can be logged by using an action in the Policy Builder, or within a style sheet. Any information you have access to when defining policies can be logged.

User-defined events are logged any time logging is enabled and are never filtered by the Identity Manager engine. You must use the policy builder to generate user-defined events.

You can specify any CEF key names in the Identity Manager policies and the specified key names will be reflected in the custom CEF event. For more information about updating the Identity Manager policies, see the *NetIQ Identity Manager - Using Designer to Create Policies*.

If you want to modify the custom CEF events, you can modify the Universal CEF collector to service the events:

1. Download and extract the latest Universal CEF collector from the Sentinel plug-ins website.
2. From the extracted folder, modify the following files:
   - `NetIQ_IDM_taxonomy.map` - To customize the taxonomy for the user defined events.
   - `NetIQ_Identity.Manager.map` - To add and map new CEF fields to Sentinel fields.
   - `idm.js` - To modify the Record.prototype.processCustomEvents(e) function.

For more information, follow the steps mentioned in Sentinel plug-ins documentation.

You can download the Sentinel plug-ins from the Sentinel download page. For more information about upgrading an existing collector, see Upgrade Procedures.

Using Policy Builder to Generate Events

1. In the Policy Builder, define the condition that must be met to generate the event, then select the **Generate Event** action.
2. Specify an event ID.

   Event IDs between 1000 and 1999 are allotted for user-defined events. You must specify a value within this range for the event ID when defining your own events. However, the event IDs between 1200 to 1203 are reserved for account related entitlement events and must not be used.

   The IDM event ID is combination of 30 and the hexadecimal of event ID.

   For example, if the ID provided in generate event policy action was 1344, then the IDM event ID is, ”30” “hexadecimal of (1344)” = “30” “540” = “30540”.
3. Select a log level.

   Log levels enable you to group events based on the type of event being logged. The following predefined log levels are available:

Log Level	Severity	Description
log-emergency	10	Events that cause the Identity Manager engine or driver to shut down.
log-alert	9	Events that require immediate attention.
log-critical	8	Events that can cause parts of the Identity Manager engine or driver to malfunction.
log-error	7	Events describing errors that can be handled by the Identity Manager engine or driver.
log-warning	4	Negative events not representing a problem.
log-notice	2	Positive or negative events an administrator can use to understand or improve use and operation.
log-info	1	Positive events of any importance.
log-debug	0	Events of relevance for support or for engineers to debug the Identity Manager engine or driver.

4 Click the icon next to the **Enter Strings** field to launch the Named String Builder.

In the Named String Builder, you can specify any key and value pair. The output will display these values as the CEF extension fields for the event.

For more information and examples of the Generate Event action, see "Generate Event" in the *NetIQ Identity Manager - Using Designer to Create Policies* guide.

eDirectory Objects that Store Identity Manager Event Data

The Identity Manager events you want to log are stored in the DirXML-LogEvents attribute on the Driver Set object or Driver object. The attribute is a multi-value integer with each value identifying an event ID to be logged.

You do not need to modify these attributes directly, because these objects are automatically configured based on your selections in iManager.

Before logging an event, the engine checks the current event type against the content of the DirXML-LogEvents attribute to determine whether the event should be logged.

Drivers can inherit log settings from the driver set. The DirXML-DriverTraceLevel attribute of a Driver object has the highest precedence when determining log settings. If a Driver object does not contain a DirXML-DriverTraceLevel attribute, the engine uses the log settings from the parent driver set.

8 Using Status Logs

In addition to the functionality provided by Sentinel, Identity Manager logs a specified number of events on the driver set and the driver. These status logs provide a view of recent Identity Manager activity. After the log reaches the set size, the oldest half of the log is permanently removed to clear room for more recent events. Therefore, any events you want to track over time should be logged to Sentinel.

The following sections contain information on the Identity Manager logs:

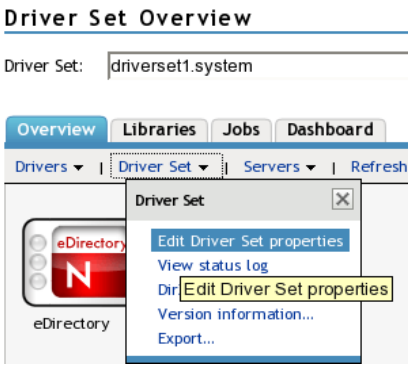
Setting the Log Level and Maximum Log Size

Status logs can be configured to hold between 50 and 500 events. This setting can be configured for the driver set to be inherited by all drivers in the driver set, or configured for each driver in the driver set. The maximum log size operates independently of the events you have selected to log, so you can configure the events you want to log for the driver set, then specify a different log size for each driver in the set.

This section reviews how to set the maximum log size on the driver set or an individual driver:

Setting the Log Level and Log Size for the Driver Set

1. In iManager, select **Identity Manager > Identity Manager Overview**.
2. Browse to and select the driver set.
3. Click the driver set name to access the driver set overview page.
4. Select **Driver Set > Edit Driver Set properties**.

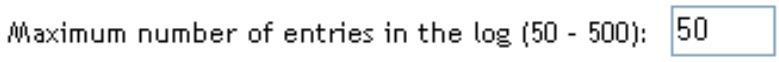


5. Select **Log Level**.

6 Enable the **Turn off logging to Driver Set, Subscriber and Publisher logs** option to prevent logging audit events to eDirectory.

   Enabling this option improves the performance of the Identity Manager system.

7 Specify the maximum log size in the **Maximum number of entries in the log** field:



8 After you have specified the maximum number, click **OK**.

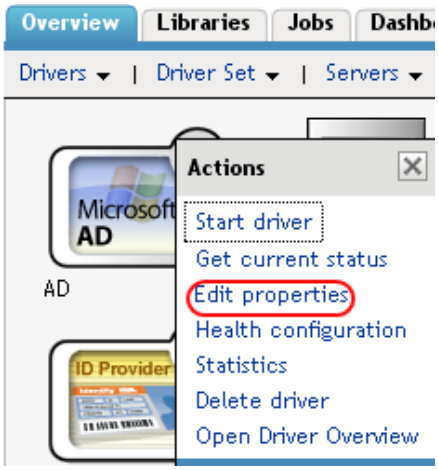
Setting the Log Level and Log Size for the Driver

1 In iManager select **Identity Manager > Identity Manager Overview**.

2 Browse to and select the driver set.

3 Click the driver set to access the driver set overview page.

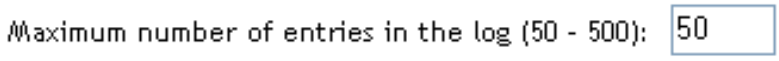
4 Click the upper right corner of the driver icon, then select **Edit properties**.



5 Select **Log Level**.

6 Deselect **Use log settings from the driver set** option, if it is selected.

7 Specify the maximum log size in the **Maximum number of entries in the log** field:



8 After you have specified the maximum number, click **OK**.

Viewing Status Logs

The status logs are short-term logs for the driver set, the Publisher channel, and the Subscriber channel. They are accessed through different locations in iManager.

- "Accessing the Driver Set Status Log" on page 39
- "Accessing the Publisher Channel and Subscriber Channel Status Logs" on page 40

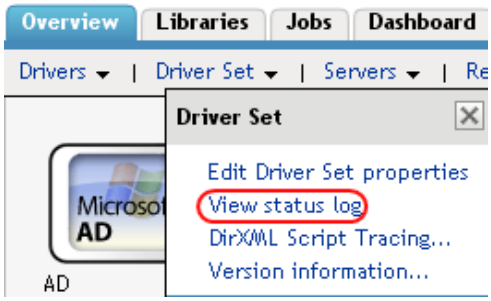
Accessing the Driver Set Status Log

The status log for the driver set contains only messages generated by the engine, such as state changes for any drivers in the driver set. All engine messages are logged. There are two ways to access the driver set status log:

- “Viewing the Log from the Driver Set Overview Page” on page 39
- “Viewing the Log from the Driver Overview Page” on page 39

Viewing the Log from the Driver Set Overview Page

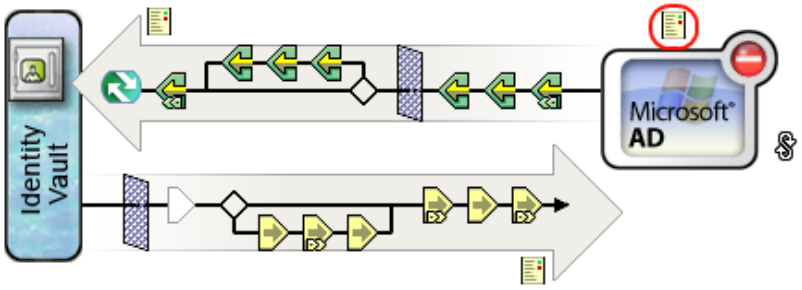
1. In iManager, select **Identity Manager > Identity Manager Overview**.
2. Browse to and select the driver set.
3. Click the driver set to access the driver set overview page.
4. Select **Driver Set > View status log**.



Viewing the Log from the Driver Overview Page

1. In iManager, select **Identity Manager > Identity Manager Overview**.
2. Browse to and select the driver set.
3. Click the driver set to access the driver set overview page, then click any driver.

   The status log for the driver is stored on the driver overview page for each driver.
4. Click the Driver Set Status Log icon above the driver object.

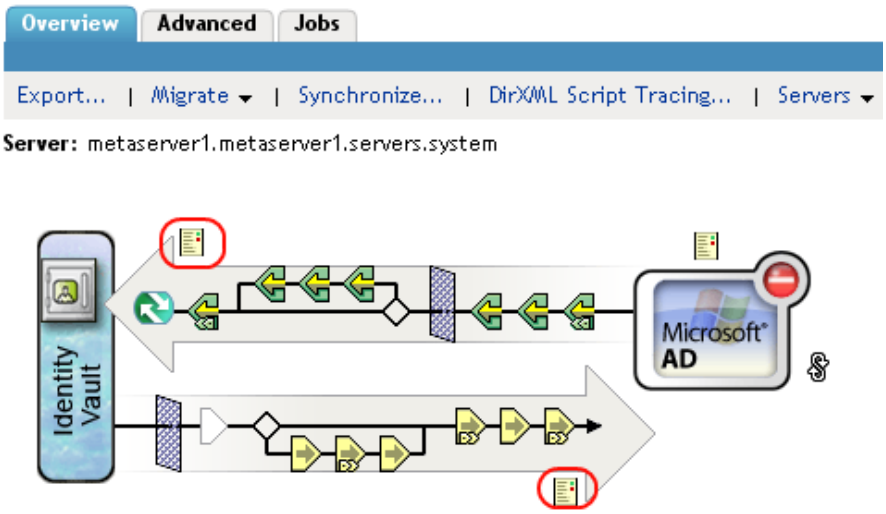


Accessing the Publisher Channel and Subscriber Channel Status Logs

The status logs for the Publisher and Subscriber channels report channel-specific messages generated by the driver, such as an operation veto for an unassociated object.

To access the Publisher channel and the Subscriber channel logs:

1. In iManager, select **Identity Manager > Identity Manager Overview**.
2. Browse to and select the driver set.
3. Click the driver set to access the driver set overview page.
4. Click the desired driver object.
5. Click the Publisher channel or the Subscriber channel status log icon.



A Identity Manager Events

This section provides a listing of all events logged by Identity Manager.

Event Structure

All events logged through Sentinel have a standardized set of fields. This allows Sentinel to log events to a structured database and query events across all logging applications.

Identity Manager events provide information in the following field structure:

```
CEF:Version|Device Vendor|Device Product|Device Version|Event Number|Event
Name|Severity|Extension
```

Remote Loader Events

The following table lists the Remote Loader events that can be audited through Sentinel:

Table A-1 *Remote Loader Events*

Event ID	Description	Trigger
0030BB8	Remote Loader Start	Occurs when the Remote Loader starts.
0030BB9	Remote Loader Stop	Occurs when the Remote Loader stops.
0030BBA	Remote Loader Connection Established	Occurs when the engine establishes a TCP connection with the Remote Loader.
0030BBB	Remote Loader Connection Dropped	Occurs when the engine-to-Remote Loader connection is lost.
0030026	Command Port is already in use	Occurs when you try to start the remote loader when it is already running.
	Invalid Response to challenge during command authentication	Occurs when you specify an incorrect password.

Engine Events

The following table lists the engine events that can be audited through Sentinel:

Table A-2 *Engine Events*

Event ID	Description	Trigger
0030001	Status Success	Many different events can cause the status success event to occur. It usually signifies that an operation was successfully completed.
0030002	Status Retry	Many different events can cause the status retry event to occur. It signifies an operation was not completed and the operation must be tried again later.
0030003	Status Warning	Many different events can cause the status warning event to occur. It usually signifies that an operation was completed with minor problems.
0030004	Status Error	Many different events can cause the status error event to occur. It usually signifies that an operation was not completed successfully.
0030005	Status Fatal	Many different events can cause the status fatal event to occur. It usually signifies that an operation was not completed successfully and the engine or driver could not continue.
0030006	Status Other	Any status document processed with a level other than the five previously defined creates a status other event. These events can only be generated within a style sheet or rule.
0030007	Search	Occurs when a query document is sent to the Identity Manager engine or driver.
0030008	Add Entry	Occurs when an object is added.
0030009	Delete Entry	Occurs when an object is deleted.
003000A	Modify Entry	Occurs when an object is modified.
003000B	Rename Entry	Occurs when an object is renamed.
003000C	Move Entry	Occurs when an object is moved.
003000D	Add Association	Occurs when an association is added. It can happen on an add or a match.
003000E	Remove Association	When an object is deleted, there is no remove association event. The remove association occurs when a User object is deleted in the disparate application, and the delete is then converted into a modify that removes the association.
003000F	Query Schema	Occurs when a query schema operation is sent to the Identity Manager engine or driver.
0030010	Check User Password Status	Manual function that is initiated via iManager to check the status of the user’s password.
0030011	Check Object Password	Occurs when a request is issued to check an object's password, other than the driver.

Event ID	Description	Trigger
00307D7	Keyed Password Set	Occurs when a named password is modified. The following sub-event types for Keyed Password Set can be found under the `act` field of the CEF event: ◆ SET_NAMED_PASSWORD ◆ CLEAR_NAMED_PASSWORD ◆ CLEAR_ALL_NAMED_PASSWORD ◆ READ_ALL_NAMED_PASSWORD_KEYS ◆ SET_NAMED_PASSWORD ◆ READ_ALL_NAMED_PASSWORD_KEYS_WITH_DISPLAY_STRINGS ◆ SET_UTF8_NAMED_PASSWORD
0030012	Change Password	Occurs when a request is issued to change the driver's password.
0030013	Sync	Occurs when a sync event is requested.
0030014	Input XML Document	Generated whenever an input document is created by the engine or driver.
0030015	Input Transformation Document	Generated after the input transformation policies are processed, allowing the user to view the transformed document.
0030016	Output Transformation Document	Generated after the output transformation policies are processed, allowing the user to view the transformed document.
0030017	Event Transformation Document	Generated after the event transformation policies are processed, allowing the user to view the transformed document.
0030018	Placement Rule Transformation Document	Generated after the Placement rule policies are processed, allowing the user to view the transformed document.
0030019	Create Rule Transformation Document	Generated after the Create rule policies are processed, allowing the user to view the transformed document.
003001A	Input Mapping Rule Transformation Document	Generated after the Schema Mapping rules are processed which convert the document to the eDirectory schema.
003001B	Output Mapping Rule Transformation Document	Generated after the Schema Mapping rules are processed which convert the document to the applications schema.
003001C	Matching Rule Transformation Document	Generated after the Matching rule policies are processed, allowing the user to view the transformed document.
003001D	Command Transformation Document	Generated after the command transformation policies are processed, allowing the user to view the transformed document.

Event ID	Description	Trigger
003001E	Publisher Filter Transformation Document	Generated after processing the notify filter on the Publisher channel, allowing the user to view the transformed document.
003001F	User Agent Request	Occurs when a User Agent XDS command document is sent to the Driver on the Subscriber channel.
0030020	Resync Driver	Occurs when a resync request is issued.
0030021	Migrate	Occurs when a migrate request is issued.
0030022	Driver Start	Occurs when a driver is started. **NOTE:** The CEF event displayed on the auditing server such as Sentinel does not fetch the Hostname/IP address details of iManager or Designer from where the driver was started.
0030023	Driver Stop	Occurs when a driver is stopped. **NOTE:** The CEF event displayed on the auditing server such as Sentinel does not fetch the Hostname/IP address details of iManager or Designer from where the driver was stopped.
0030024	Password Sync	Generated when setting the distribution or simple password on an object.
0030025	Password Reset	Generated when resetting the connected application password after a failed password sync operation.
0030026	DirXML Error	Generated whenever the engine throws an internal error.
0030027	DirXML Warning	Generated whenever the engine throws an internal warning.
0030028	Custom Operation	Occurs when an unknown operation appears in an input document. An example of known operations would be an add, delete, or modify.
0030029	Clear Attribute	Occurs when a modify operation contains a remove-all-value element.
003002A	Add Value - Modify Entry	Occurs when a value is added during the modification of an object.
003002B	Remove Value	Occurs when a modify operation contains a remove-value element.
003002C	Merge Entries	Occurs when two objects are being merged.
003002D	Get Named Password	Generated on a Get Named Password operation.
003002E	Reset Attributes	Occurs when a Reset document is issued on the publisher or Subscriber channels.
003002F	Add Value - Add Entry	Occurs when a value is added during the creation of an object.
0030030	Set SSO Credential	Occurs when a driver policy executes the do-set-sso-credential action.
0030031	Clear SSO Credential	Occurs when a driver policy executes the do-clear-sso-credential action.
0030032	Set SSO Passphrase	Occurs when a driver policy executes the do-clear-sso-credential action.

Event ID	Description	Trigger
0030033	Startup Rule	Generated after the Startup policies are processed. Allows the user to view the transformed document.
0030034	Shutdown Rule	Generated after the Shutdown policies are processed. Allows allows the user to view the transformed document.
0030035	Send Mail	Occurs when a policy or job is executed where the send mail option is configured. This will trigger a job to send an e-mail.
0030036	Entitlement Operation	Occurs when the value of the DirXML-EntitmentResult changes.
000304B0	Account Create By Entitlement Grant	Occurs when an account is created by granting of an entitlement.
000304B1	Account Delete By Entitlement Revoke	Occurs when an account is deleted on revoking of the entitlement.
000304B2	Account Disable By Entitlement Revoke	Occurs when an account is disabled on revoking of the entitlement.
000304B3	Account Enable By Entitlement Grant	Occurs when an account is enabled by granting of an entitlement.

Fanout Agent Events

The following table lists the Fanout Agent events that can be audited through Sentinel:

Table A-3 *Fanout Agent Events*

Event ID	Description	Trigger
0030FA0	Fanout Agent Start	Occurs when the Fanout Agent starts.
0030FA1	Fanout Agent Stop	Occurs when the Fanout Agent stops.
0030FA2	Service Start, Instance Service	Occurs when the driver is started
0030FA3	Service Stop, Instance Service	Occurs when the driver is stopped.

Identity Applications Events

The following table lists the User Application events that can be audited through Sentinel:

Table A-4 *User Application Events*

Event ID	Description	Trigger
31400	Delete Entity	Occurs when an entity is deleted
31401	Update Entity	Occurs when an entity is updated

Event ID	Description	Trigger
31550	Login Success	Occurs when the login succeeds
31551	Login Failure	Occurs when the login fails
31440	Create Entity	Occurs when an entity is created
31450	Create Proxy Definition Success	Occurs when the creation of an entity definition succeeds
31451	Create Proxy Definition Failure	Occurs when the creation of an proxy definition fails
31452	Update Proxy Definition Success	Occurs when an update to the proxy definition fails
31453	Update Proxy Definition Failure	Occurs when an update to the proxy definition fails
31454	Delete Proxy Definition Success	Occurs when the proxy definition is deleted successfully
31455	Delete Proxy Definition Failure	Occurs when the proxy definition is not deleted successfully
31456	Create Delegatee Definition Success	Occurs when the creation of a delegatee definition succeeds
31457	Create Delegatee Definition Failure	Occurs when the creation of a delegatee definition fails
31458	Update Delegatee Definition Success	Occurs when an update to the delegatee definition succeeds
31459	Update Delegatee Definition Failure	Occurs when an update to the delegatee definition fails
003145A	Delete Delegatee Definition Success	Occurs when the delegatee definition is deleted successfully
003145B	Delete Delegatee Definition Failure	Occurs when the deletion of a delegatee definition fails
003145C	Create Availability Success	Occurs when the creation of an availability succeeds
003145D	Create Availability Failure	Occurs when the creation of an availability fails
3145	Delete Availability Success	Occurs when the deletion of an availability succeeds
003145F	Delete Availability Failure	Occurs when the deletion of an availability fails
31520	Workflow Error	Occurs when there is a workflow error
31521	Workflow Started	Occurs when the workflow starts
31522	Workflow Forwarded	Occurs when the workflow is forwarded
31523	Workflow Reassigned	Occurs when the workflow is reassigned
31524	Workflow Approved	Occurs when the workflow is approved
31525	Workflow Refused	Occurs when the workflow is refused

Event ID	Description	Trigger
31526	Workflow Ended	Occurs when the workflow ends
31527	Workflow Claimed	Occurs when the workflow is claimed
31528	Workflow Unclaimed	Occurs when the workflow is not claimed
31529	Workflow Denied	Occurs when the workflow is denied
003152A	Workflow Completed	Occurs when the workflow is completed
003152B	Workflow Timedout	Occurs when the workflow timed out
003152C	User Message	This is a user adhoc log message
003152D	Provision Error	Occurs when there is an error in the provisioning step
3152E	Provision Submitted	Occurs during the provisioning step on submission of entitlements.
003152F	Provision Success	Occurs during the provisioning step on successful completion of the step
31530	Provision Failure	Occurs during the provisioning step upon failure of the step
31531	Provision Granted	Occurs during the provisioning step on granting of an entitlement
31532	Provision Revoked	Occurs during the provisioning step on the revoking of an entitlement
31533	Workflow Retracted	Occurs when the workflow is retracted
31534	Workflow Escalated	Occurs when the workflow is escalated
31535	Workflow Reminder Sent	Occurs when reminders are sent to addressees of a workflow task
31536	Digital Signature	Occurs whenever a digital signature is passed to the workflow engine
31537	Workflow ResetPriority	Occurs when the priority of a workflow task is reset.
31538	Role Approved	Occurs when a role is approved
31539	Role Denied	Occurs when a role is denied
003153A	SOD Exception Approved	Occurs when an SOD exception is approved
003153B	SOD Exception Denied	Occurs when an SOD exception is denied
003153C	Start Correlated Workflow	Occurs when a correlated workflow is started
003153D	Role Request Submitted	Occurs when a role request is submitted
3153	Resource Approved	Occurs when a resource is approved
003153F	Resource Denied	Occurs when a resource is denied
31540	Provision Already Exists	
31541	Resource Request Submitted	Occurs when a request for a resource is submitted
31542	Resource Provisioning Workflow Submitted	Occurs when a resource provisioning workflow is submitted
31543	Resource Provisioning Workflow Failed	Occurs when a resource provisioning workflow fails
31600	Role Provisioning	Occurs when a role is provisioned

Event ID	Description	Trigger
31601	Role Provisioning Failure	Occurs when a role provisioning fails
31610	Role Request	Occurs when a role is requested
31611	Role Request Failure	Occurs when the request for a role fails
31612	Role Request Workflow	
31613	SOD Exception Auto Approval	Occurs when the SOD exception is auto approved
31614	Retract Role Request	Occurs when the role request is retracted
31615	Retract Role Request Failure	Occurs when the retraction of a role request fails
31620	Entitlement Grant	Occurs when the entitlement is granted
31621	Entitlement Grant Failure	Occurs when the entitlement grant fails
31622	Entitlement Revoke	Occurs when the entitlement is revoked
31623	Entitlement Revoke Failure	Occurs when the entitlement revoke fails
31694	Create Authorization	Occurs when the permissions are assigned to the team
31695	Delete Authorization	Occurs when the permissions are removed from the team

Identity Reporting Events

The following table lists Identity Reporting events that can be audited through Sentinel:

Table A-5 *Identity Reporting Events*

Event ID	Description	Trigger
00031771	Report Created	Occurs when the report is added
00031772	Report Modified	Occurs when the report is modified
00031773	Report Deleted	Occurs when the report is deleted
00031774	Schedule Created	Occurs when the schedule is created
00031775	Schedule Modified	Occurs when the schedule is modified
00031776	Schedule Deleted	Occurs when the schedule is deleted
00031777	Report Generated	Occurs when the report is generated
00031778	Report Delivered	Occurs when the report is delivered

DCS Events

The following table lists Data Collection Service events that can be audited through Sentinel:

Table A-6 *DCS Events*

Event ID	Description	Trigger
00031721	DCS Driver Registration Add	Occurs when the DCS driver is added
00031722	DCS Driver Registration Modify	Occurs when the DCS driver is modified
00031723	DCS Driver Collection enabled	Occurs when the data collection is enabled
00031724	DCS Driver Collection disabled	Occurs when the data collection is disabled
00031728	Data Collection Suspended	Occurs when the data collection is suspended
00031729	Data Collection Activated	Occurs when the data collection is activated
00031730	Data Collection Started	Occurs when the data collection is started
00031731	Data Collection Completed	Occurs when the data collection is completed
00031732	Data Collection Failed	Occurs when the data collection fails
00031733	Data Collection Requested	Occurs when the data collection is requested
00031734	Data Cleanup Requested	Occurs when the data cleanup is requested
00031735	Data Cleanup Started	Occurs when the data cleanup is started
00031736	Data Cleanup Completed	Occurs when the data cleanup is completed
00031736	Data Cleanup Failed	Occurs when the data cleanup fails

B Understanding the Properties Files for CEF Auditing

The appendix provides details about the properties files used by the different components of Identity Manager for auditing through CEF.

Understanding the auditlogconfig.properties File

The following Identity Manager components use `auditlogconfig.properties` file to store the CEF configuration:

- Identity Vault
- Identity Manager Engine
- Java Remote Loader
- Fanout Agent

For information about the content of the audit properties file for each of these Identity Manager components, see the following sections:

- "Identity Manager Engine, Remote Loader, and .NET Remote Loader" on page 51
- "Java Remote Loader and Fanout Agent" on page 54

Identity Manager Engine, Remote Loader, and .NET Remote Loader

The following is a sample `auditlogconfig.properties` file for Identity Manager engine, Remote Loader, and .NET Remote Loader:

```
# Set the level of the root logger to DEBUG and attach appenders.
#log4j.rootLogger=debug, S, R

# Defines appender S to be a SyslogAppender.
#log4j.appender.S=org.apache.log4j.net.SyslogAppender

# Defines location of Syslog server.
#log4j.appender.S.Host=localhost
#log4j.appender.S.Port=port

# Specify protocol to be used (UDP/TCP/SSL)
#log4j.appender.S.Protocol=SSL

# Specify SSL certificate file for SSL connection.
# File path should be given with double backslash.
#log4j.appender.S.SSLCertFile=/etc/opt/novell/mycert.pem

# Minimum log-level allowed in syslog.
#log4j.appender.S.Threshold=INFO
```

```
# Defines the type of facility.
#log4j.appender.S.Facility=USER

# Defines caching for SyslogAppender.
# Inputs should be yes/no
#log4j.appender.S.CacheEnabled=yes

# Cache location directory
# Directory should be available for creating cache files
#log4j.appender.S.CacheDir=/var/opt/novell/eDirectory

# Cache File Size
# Cache File size should be in the range of 50MB to 4000MB
#log4j.appender.S.CacheMaxFileSize=500MB

# Layout definition for appender Syslog S.
#log4j.appender.S.layout=org.apache.log4j.PatternLayout
#log4j.appender.S.layout.ConversionPattern=%c: %m%n

# Defines appender R to be a Rolling File Appender.
#log4j.appender.R=org.apache.log4j.RollingFileAppender

# Log file for appender R.
#log4j.appender.R.File=/var/opt/novell/eDirectory/log/cef-events.log

# Max size of log file for appender R.
#log4j.appender.R.MaxFileSize=100MB

# Set the maximum number of backup files to keep for appender R.
# Max can be 13. If set to zero, then there will be no backup files.
#log4j.appender.R.MaxBackupIndex=10

# Layout definition for appender Rolling log file R.
#log4j.appender.R.layout=org.apache.log4j.PatternLayout
#log4j.appender.R.layout.ConversionPattern=%d{MMM dd HH:mm:ss} %c %m%n
```

NOTE: By default, the appenders are disabled. You need to manually enable them.

Before using the `auditlogconfig.properties` file, NetIQ recommends you to review the following considerations:

- The letters S and R specify Syslog Appender and Rolling File Appender respectively.
- Entries in the `auditlogconfig.properties` file are not case sensitive.
- Entries in the `auditlogconfig.properties` file can appear in any order.
- Empty lines in the file are valid.
- Any line that starts with a hash (#) is commented out.

The following table provides an explanation of each property in the `auditlogconfig.properties` file:

Setting	Description
log4j.rootLogger	Sets the level of the root logger to debug and attaches an appender named R or S, where S specifies a Syslog appender and R specifies a Rolling File appender.
log4j.appender.S	Specifies the appender S to be a Syslog appender.

Setting	Description
log4j.appender.S.Host	Specifies the location of the Syslog server where audit events are logged.
log4j.appender.S.Port	The port at which the Auditing server connects to the Syslog server. If the connection between Auditing server and the Syslog server fails, Identity Manager cannot log events until the connection is restored.
log4j.appender.S.Protocol	Specifies the protocol to use. For example, UDP, TCP, or SSL. SSL is the default protocol. For enabling secure communication, see Chapter 6, “Securing the Logging System,” on page 29.
log4j.appender.S.SSLCertFile	Specifies the SSL certificate file for the SSL connection. Use double backslashes to specify the path of the file. This is an optional setting.
log4j.appender.S.Threshold	Specifies the minimum log level allowed in the Syslog appender. INFO is the only supported log level.
log4j.appender.S.Facility	Specifies the type of facility.
log4j.appender.S.CacheEnabled	Specifies caching for Syslog appender.
log4j.appender.S.CacheDir	Specifies the directory for storing the cache file.
log4j.appender.S.CacheMaxFileSize	Specifies the size of the cache file. The range is 50 MB to 4000 MB.
log4j.appender.S.layout	Layout setting for Syslog appender.
log4j.appender.S.layout.ConversionPattern	Layout setting for Syslog appender.
log4j.appender.R	Specifies appender R to be a Rolling File appender.
log4j.appender.R.File	The location of the log file for a Rolling File appender.
log4j.appender.R.MaxFileSize	The maximum size, in MBs, of the log file for a Rolling File appender. Set this value to the maximum size that the client allows. This field accepts only integer value. **NOTE:** The minimum size of the `MaxFileSize` parameter for the Rolling File appender is 50 MB.
log4j.appender.R.MaxBackupIndex	Specify the maximum number of backup files for a Rolling File appender. The maximum number of the backup files can be 10. A zero value means no backup files.
log4j.appender.R.layout	Layout setting for Rolling File appender.
log4j.appender.R.layout.ConversionPattern	Layout setting for Rolling File appender.

Enabling the Syslog Appender

1. Change the following entry to S to attach a Syslog appender:

   ```
   log4j.rootLogger=debug, S
   ```

2. Uncomment the following entries:

   ```
   log4j.appender.S=org.apache.log4j.net.SyslogAppender
   ```

   ```
   log4j.appender.S.Host=localhost
   ```

```
log4j.appender.S.Port=port

log4j.appender.S.Protocol=SSL

log4j.appender.S.SSLCertFile=/etc/opt/novell/mycert.pem

log4j.appender.S.Threshold=INFO

log4j.appender.S.Facility=USER

log4j.appender.S.layout=org.apache.log4j.PatternLayout

log4j.appender.S.layout.ConversionPattern%c: =%m%n
```

3 Log in to iManager and change the log events.

For more information on changing log levels by using iManager, see “Setting the Log Level and Maximum Log Size” on page 37.

4 Restart eDirectory.

Enabling the Rolling File Appender

The Rolling File appender is preferred, if the auditing solution is limited to an individual server. Rolling file appender is more reliable compared to the Syslog appender because it uses the file connector to send events from your local file system to the auditing server.

1 Change the following entry to R to attach a Rolling File appender:

```
log4j.rootLogger=debug, R
```

2 Uncomment the following entries:

```
log4j.appender.R=org.apache.log4j.RollingFileAppender

log4j.appender.R.File=/var/opt/novell/eDirectory/log/cef-events.log

log4j.appender.R.MaxFileSize=100MB

log4j.appender.R.MaxBackupIndex=10

log4j.appender.R.layout=org.apache.log4j.PatternLayout

log4j.appender.R.layout.ConversionPattern=%d{MMM dd HH:mm:ss} %c %m%n
```

3 Log in to iManager and change log levels.

For more information on changing log levels by using iManager, see “Setting the Log Level and Maximum Log Size” on page 37.

4 Restart eDirectory.

Java Remote Loader and Fanout Agent

The following is a sample `auditlogconfig.properties` file for the Java Remote Loader and the Fanout agent.

```
# Defines location of Syslog server.
#SyslogHost=localhost
#SyslogPort=port

# Specify protocol to be used (UDP/TCP/SSL)
#SyslogProtocol=TCP

# Specify SSL keystore file for SSL connection.
# File path should be given with double backslash.
#SyslogSSLKeystoreFile=/opt/netiq/idm/jre/lib/security/cacerts

# Specify SSL keystore password for SSL connection.
#SyslogSSLKeystorePassword=password

# Defines caching for SyslogAppender.
# Inputs should be yes/no
#CacheEnabled=yes

# Cache location directory
# Directory should be available for creating cache files
#CacheDir=/tmp/IDMcache

# Cache File Size
# Cache File size should be in the range of 50MB to 4000MB
#CacheRolloverSize=50

# Log file for appender
#FileAppenderFileName=/var/opt/novell/log/cef-events.log
```

The following table provides an explanation of each property in the `auditlogconfig.properties` file:

Setting	Description
SyslogHost	Specifies the location of the Syslog server where audit events are logged.
SyslogPort	The port at which the Auditing server connects to the Syslog server. If the connection between Auditing server and the Syslog server fails, Identity Manager cannot log events until the connection is restored.
SyslogProtocol	Specifies the protocol to use. For example, UDP, TCP, or SSL.
SyslogSSLKeystoreFile	Specifies the SSL certificate file for the SSL connection. Use double backslashes to specify the path of the file. This is an optional setting.
SyslogSSLKeystorePassword	Specifies the keystore password for the SSL connection.
CacheEnabled	Specifies caching for SyslogAppender. The values can be **yes** or **no**.
CacheDir	Specifies the directory for storing the cache file.
CacheRolloverSize	Specifies the size of the cache file. The range is 50 MB to 4000 MB.
FileAppenderFileName	Specifies the log file for appender.

Setting	Description
AppendComponentName	Specifies whether you want to append the component name before the event message. You can set this option to **Yes** if you are using Sentinel as your auditing solution.

Understanding the idmuserapp_logging.xml File

The following is a sample of the `idmuserapp_logging.xml` file:

```
 <logging xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="logging-config.xsd">

    <prefix>[RBPM]</prefix>

    <!-- example of enabling TRACE level -->
    <!--
    <logger name="com.novell.soa.af" additivity="true" level="TRACE"/>
    -->
    <!--
    <logger name="com.novell" additivity="true" level="INFO">
      <appender-ref ref="CONSOLE_DEBUG"/>
    </logger>
    -->

    <!-- Appender definitions -->
    <appenders>
        <!-- CONSOLE and FILE appender are defined in jboss-log4j.xml -->
        <!-- CEF appender -->
        <appender class="com.netiq.idm.logging.syslog.CEFSyslogAppender"
name="CEF">
           <param name="Threshold" value="INFO"/>
           <param name="Facility" value="user"/>
           <param name="SyslogHost"
value="${com.netiq.ism.audit.cef.host:localhost}" />
          <param name="SyslogPort" value="${com.netiq.ism.audit.cef.port:1468}" />
           <param name="SyslogProtocol"
value="${com.netiq.ism.audit.cef.protocol:tcp}" />
           <param name="SyslogSslKeystoreFile"
value="${com.netiq.idm.audit.cef.tls-keystore:/opt/netiq/idm/apps/jre/lib/
security/cacerts}" />
           <param name="SyslogSslKeystorePassword"
value="${com.netiq.idm.audit.cef.tls-keystore-password:KeystorePassword}" />
          <param name="CacheDir" value="${com.netiq.ism.audit.cef.cache-file-dir:/
opt/netiq/idm/apps}" />
           <param name="CacheRolloverSize" value="2"/>
           <param name="ApplicationName" value="RBPM"/>
           <param name="EventPrefix" value="IDM:"/>
       </appender>
    </appenders>

    <!--
        Logger definitions

       NOTE: CONSOLE & FILE appenders should be defined in (jboss-)log4j.xml file.
        Additivity of true means the loggers defined below will inherit the
appenders.
    -->
```

```
    <loggers>
        <logger name="com.novell" level="INFO" additivity="true">
            <appender-ref ref="CEF"/>
        </logger>
        <logger name="com.sssw" level="INFO" additivity="true">
            <appender-ref ref="CEF"/>
        </logger>
        <logger name="com.netiq" level="INFO" additivity="true">
            <appender-ref ref="CEF"/>
        </logger>
        <logger name="com.novell.afw.portal.aggregation" level="INFO"
additivity="true"/>
        <logger name="com.novell.afw.portal.persist" level="INFO"
additivity="true"/>
        <logger name="com.novell.afw.portal.portlet" level="INFO"
additivity="true"/>
        <logger name="com.novell.afw.portal.util" level="INFO" additivity="true"/>
        <logger name="com.novell.afw.portlet.consumer" level="INFO"
additivity="true"/>
       <logger name="com.novell.afw.portlet.core" level="INFO" additivity="true"/>
        <logger name="com.novell.afw.portlet.persist" level="INFO"
additivity="true"/>
        <logger name="com.novell.afw.portlet.producer" level="INFO"
additivity="true"/>
       <logger name="com.novell.afw.portlet.util" level="INFO" additivity="true"/>
        <logger name="com.novell.afw.theme" level="INFO" additivity="true"/>
        <logger name="com.novell.afw.util" level="INFO" additivity="true"/>
        <logger name="com.novell.common.auth" level="INFO" additivity="true"/>
        <logger name="com.novell.idm.security.authorization.service" level="INFO"
additivity="true"/>
        <logger name="com.novell.pwdmgt.actions" level="INFO" additivity="true"/>
        <logger name="com.novell.pwdmgt.util" level="INFO" additivity="true"/>
        <logger name="com.novell.pwdmgt.service" level="INFO" additivity="true"/>
        <logger name="com.novell.pwdmgt.soap" level="INFO" additivity="true"/>
        <logger name="com.novell.roa.resources" level="INFO" additivity="true"/>
        <logger name="com.novell.soa.af.impl" level="INFO" additivity="true"/>
        <logger name="com.novell.soa.script" level="INFO" additivity="true"/>
        <logger name="com.novell.soa.ws.impl" level="INFO" additivity="true"/>
        <logger name="com.novell.srvprv.apwa" level="INFO" additivity="true"/>
        <logger name="com.novell.srvprv.impl.portlet" level="INFO"
additivity="true"/>
        <logger name="com.novell.srvprv.impl.portlet.util" level="INFO"
additivity="true"/>
        <logger name="com.novell.srvprv.impl.servlet" level="INFO"
additivity="true"/>
        <logger name="com.novell.srvprv.impl.uictrl" level="INFO"
additivity="true"/>
        <logger name="com.novell.srvprv.impl.vdata.model" level="INFO"
additivity="true"/>
        <logger name="com.novell.srvprv.impl.vdata.definition" level="INFO"
additivity="true"/>
        <logger name="com.novell.srvprv.spi" level="INFO" additivity="true"/>
        <logger name="com.sssw.fw.cachemgr" level="INFO" additivity="true"/>
        <logger name="com.sssw.fw.core" level="INFO" additivity="true"/>
        <logger name="com.sssw.fw.directory" level="INFO" additivity="true"/>
        <logger name="com.sssw.fw.event" level="INFO" additivity="true"/>
        <logger name="com.sssw.fw.factory" level="INFO" additivity="true"/>
        <logger name="com.sssw.fw.persist" level="INFO" additivity="true"/>
        <logger name="com.sssw.fw.resource" level="INFO" additivity="true"/>
        <logger name="com.sssw.fw.security" level="INFO" additivity="true"/>
```

```
        <logger name="com.sssw.fw.server" level="INFO" additivity="true"/>
        <logger name="com.sssw.fw.servlet" level="INFO" additivity="true"/>
        <logger name="com.sssw.fw.session" level="INFO" additivity="true"/>
        <logger name="com.sssw.fw.usermgr" level="INFO" additivity="true"/>
        <logger name="com.sssw.fw.util" level="INFO" additivity="true"/>
        <logger name="com.sssw.portal.manager" level="INFO" additivity="true"/>
        <logger name="com.sssw.portal.persist" level="INFO" additivity="true"/>
        <logger name="com.novell.idm.nrf.persist" level="INFO" additivity="true"/>
        <logger name="com.novell.idm.nrf.service" level="INFO" additivity="true"/>
        <logger name="com.novell.srvprv.impl.uictrl" level="INFO"
additivity="true"/>
       <logger name="com.novell.srvprv.spi.uictrl" level="INFO" additivity="true"/
>
    </loggers>
</logging>
```

Understanding the workflow_logging.xml File

The following is a sample of the `workflow_logging.xml` file:

```
<logging xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="logging-config.xsd">

    <prefix>[WORKFLOW]</prefix>

    <!-- example of enabling TRACE level -->
    <!--
    <logger name="com.novell.soa.af" additivity="true" level="TRACE"/>
    -->
    <!--
    <logger name="com.novell" additivity="true" level="INFO">
      <appender-ref ref="CONSOLE_DEBUG"/>
    </logger>
    -->

    <!-- Appender definitions -->
    <appenders>
        <!-- CONSOLE and FILE appender are defined in jboss-log4j.xml -->
        <!-- CEF appender -->

        <appender class="com.netiq.idm.logging.syslog.CEFSyslogAppender"
name="WFCEF">
            <param name="Threshold" value="INFO"/>
            <param name="Facility" value="user"/>
            <param name="SyslogHost"
value="${com.netiq.ism.audit.cef.host:localhost}" />
           <param name="SyslogPort" value="${com.netiq.ism.audit.cef.port:1468}" /
>
            <param name="SyslogProtocol"
value="${com.netiq.ism.audit.cef.protocol:tcp}" />
            <param name="SyslogSslKeystoreFile"
value="${com.netiq.idm.audit.cef.tls-keystore:/opt/netiq/idm/apps/jre/lib/
security/cacerts}" />
            <param name="SyslogSslKeystorePassword"
value="${com.netiq.idm.audit.cef.tls-keystore-password:KeystorePassword}" />
            <param name="CacheDir" value="${com.netiq.ism.audit.cef.cache-file-
dir:/opt/netiq/idm/apps}" />
            <param name="CacheRolloverSize" value="2"/>
            <param name="ApplicationName" value="WORKFLOW"/>
```

```
            <param name="EventPrefix" value="IDM:"/>
        </appender>
</appenders>

    <!--
        Logger definitions
NOTE: CONSOLE & FILE appenders should be defined in (jboss-)log4j.xml file.
        Additivity of true means the loggers defined below will inherit the
appenders.
    -->
    <loggers>
        <logger name="workflow.log" level="INFO" additivity="true">
            <appender-ref ref="WFCEF"/>
        </logger>
        <logger name="com.novell" level="INFO" additivity="true">
            <appender-ref ref="WFCEF"/>
        </logger>
        <logger name="com.netiq" level="INFO" additivity="true">
            <appender-ref ref="WFCEF"/>
        </logger>
        <logger name="com.sssw" level="INFO" additivity="true">
            <appender-ref ref="WFCEF"/>
        </logger>
        <logger name="com.microfocus" level="INFO" additivity="true">
            <appender-ref ref="WFCEF"/>
        </logger>
    </loggers>
   <root>
    <priority value="INFO"/>
  </root>
</logging>
```

Understanding the idmrptdcs_logging.xml File

The following is a sample of the `idmrptdcs_logging.xml` file:

```
<logging>
<!-- Prefix for logging messages from this logger configuration -->
<prefix>[DCS-CORE]</prefix>
<loggers>
    <logger additivity="true" name="com.novell" level="INFO">
    </logger>
    <logger additivity="true" name="com.netiq" level="INFO">
    </logger>
</loggers>
<audit>
    <!--Defines location of Syslog server.-->
    <!--
    <SyslogHost>127.0.0.1</SyslogHost>
    <SyslogPort>1468</SyslogPort>
    -->
    <!--Specify protocol to be used (UDP/TCP/SSL)-->
    <!--
    <SyslogProtocol>TCP</SyslogProtocol>
    -->

    <!--Specify SSL keystore file for SSL connection.
    ~ File path should be given with double backslash.
    -->
```

```
    <!--For Linux-->
    <!--
    <SyslogSSLKeystoreFile>/etc/opt/novell/mycert.pem</SyslogSSLKeystoreFile>
    -->
    <!--For Windows, file path should be given with double backslash.-->
    <!--
    <SyslogSSLKeystoreFile>C:\\Novell\\mycert.pem</SyslogSSLKeystoreFile>
    -->

    <!--Specify SSL keystore password for SSL connection. -->
    <!--
    <SyslogSSLKeystorePassword>password</SyslogSSLKeystorePassword>
    -->

    <!--Specify whether to append the component name before the event message
    ~ Inputs should be yes/no
    ~ If NetIQ Sentinel is the event listener, this option should be set to 'yes'
    -->
    <!--
    <AppendComponentName>yes</AppendComponentName>
    -->

    <!--Defines caching for SyslogAppender.
    ~ Inputs should be yes/no
    -->
    <!--
    <CacheEnabled>yes</CacheEnabled>
    -->

    <!--Cache location Directory
    ~ Directory should be available for creating cache files
    ~ Directory should have 'novlua' permission for caching to work correctly
    -->
    <!--For Linux-->
    <!--
    <CacheDir>/var/opt/netiq/idm/dcs-cache</CacheDir>
    -->
    <!--For Windows, file path should be given with double backslash.-->
    <!--
    <CacheDir>C:\\NetIQ\\idm\\IDMcache</CacheDir>
    -->

    <!--Cache File Size
    ~ Cache File size should be in the range of 50MB to 4000MB
    -->
    <!--
    <CacheRolloverSize>50</CacheRolloverSize>
    -->

    <!--Log file for appender
    ~ The directory containing the file specified should have 'novlua' permission
to work correctly.
    -->
   <!--For Linux-->
    <!--
```

```
    <FileAppenderFileName>/var/opt/netiq/idm/dcs-cache/cef-events.log</
FileAppenderFileName>
    -->
    <!--For Windows, file path should be given with double backslash.-->
    <!--
    <FileAppenderFileName>C:\\cef-events.log</FileAppenderFileName>
    -->

    <!--Max size of log file for file appender -->
    <!--
    <FileMaxRolloverSize>50</FileMaxRolloverSize>
    -->
</audit>
</logging>
```

NOTE: By default, the appenders are disabled. You need to manually enable them by uncommenting the appender section.

Understanding the idmrptcore_logging.xml File

The following is a sample of the `idmrptcore_logging.xml` file:

```
<logging xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="logging-config.xsd">

<!-- Prefix for logging messages from this logger configuration -->
<prefix>[RPT-CORE]</prefix>

<audit>
        <syslog>
            <enabled>${com.netiq.ism.audit.cef.enabled:false}</enabled>
            <protocol>${com.netiq.ism.audit.cef.protocol:TCP}</protocol>
            <host>${com.netiq.ism.audit.cef.host:localhost}</host>
            <port>${com.netiq.ism.audit.cef.port:514}</port>
            <cache-dir>${com.netiq.ism.audit.cef.cache-file-dir:/tmp/rpt-syslog-
cache}</cache-dir>
            <cache-file>idm-rpt</cache-file>
            <application>Identity Manager Reporting</application>
            <vendor>Micro Focus</vendor>
            <version>6.5.0</version>
            <keystore-file>${com.netiq.idm.osp.ssl-keystore.file:/tmp/
keystore.jks}</keystore-file>
            <keystore-password>${com.netiq.idm.osp.ssl-keystore.pwd:changeit}</
keystore-password>
            <keystore-type>${com.netiq.idm.osp.ssl-keystore.type:JKS}</keystore-
type>
```

```
            </syslog>
        </audit>

        <!-- Logger definitions -->
        <loggers>
            <!-- Example of enabling TRACE level -->
            <!--
            <logger additivity="true" name="com.novell.soa.af" level="TRACE"/>
            -->
            <logger additivity="true" name="com.novell" level="INFO"/>
            <logger additivity="true" name="com.netiq" level="INFO"/>
        </loggers>

    </logging>
```

9 Troubleshooting

This section provides useful information for troubleshooting problems with CEF Auditing.

Error on Identity Manager Dashboard Login Page

During the audit configuration, if the *novlua* permissions are not set for the Intermediate event store directory, then you will see the following error on login page of Identity Manager Dashboard.

```
{"Fault":{"Code":["Value":"Sender","Subcode":{"Value":"XDAS_OUT_FAILURE"}},"Reason
":{"Text":"System not in a fully started state. (perhaps starting, shutting down,
refreshing configuration, or restarting)"}}}
```

Perform the following actions to resolve this error:

1. Change the permission of the intermediate event store directory by running the commands:

   ```
   chown novlua:novlua <directory_path>
   ```

   ```
   chmod 755 <directory_path>
   ```

   where `<directory_path>` is path to the intermediate event store directory.
2. Restart the Tomcat service.
3. Disable the CEF audit configuration using configuration update utility and restart the tomcat service. Now carefully repeat the configuration steps to enable CEF auditing.